

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-351744

(43)Date of publication of application : 06.12.2002

(51)Int.Cl.

G06F 12/14  
H04L 9/08

(21)Application number : 2001-161234

(71)Applicant : SONY CORP

(22)Date of filing : 29.05.2001

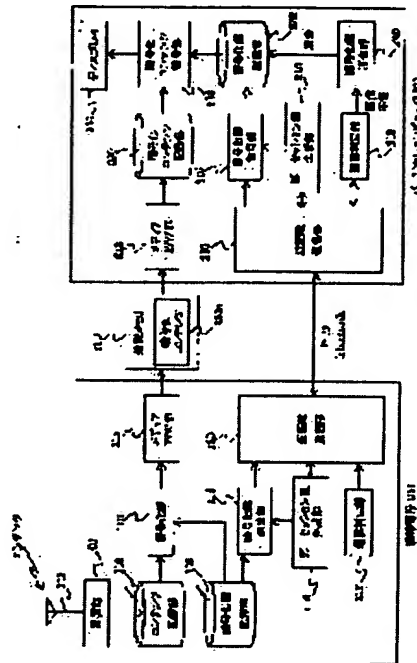
(72)Inventor : SAWADA TAKESHI

(54) CONTENTS RECORDING SYSTEM, DEVICE, METHOD AND PROGRAM FOR CONTENTS TRANSFER, AND RECORDING MEDIUM HAVING THE SAME PROGRAM RECORDED THEREON

(57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a contents recording system which can legally move contents out of a portable telephone when the contents are recorded on the portable telephone.

**SOLUTION:** The contents recorded in a contents recording part 106 are ciphered by a ciphering part 110 and transferred to a ciphered contents recording part 230 through a detachable memory 300. When a communication decision part 218 decides that short-distance communication with the portable telephone 100 is possible, a ciphered contents decoding part 234 deciphers the ciphered contents, and hence the contents are made usable. When a 3rd person tries to illegally copy the contents, the portable telephone 100 and a personal computer 200 are put far away from each other and the communication decision part 218 becomes unable to perform the short-distance communication with the portable telephone 100. In this case, a ciphering key erasure part 240 erases the ciphering key recorded in a ciphering key recording part 232, so the ciphered contents cannot be deciphered to prevent the contents from being illegally copied.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision]

of rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-351744

(P2002-351744A)

(43) 公開日 平成14年12月6日 (2002.12.6)

(51) Int.Cl.<sup>7</sup>

識別記号

F I

テーマコード(参考)

G 0 6 F 12/14

3 2 0

G 0 6 F 12/14

3 2 0 E 5 B 0 1 7

H 0 4 L 9/08

H 0 4 L 9/00

6 0 1 B 5 J 1 0 4

6 0 1 A

審査請求 未請求 請求項の数 8 O L (全 8 頁)

(21) 出願番号 特願2001-161234(P2001-161234)

(22) 出願日 平成13年5月29日 (2001.5.29)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 澤田 健

東京都品川区北品川6丁目7番35号 ソニ

ー株式会社内

(74) 代理人 100097490

弁理士 細田 益穂

Fターム(参考) 5B017 AA07 BA07 CA14

5J104 AA01 AA16 EA17 NA02 NA37

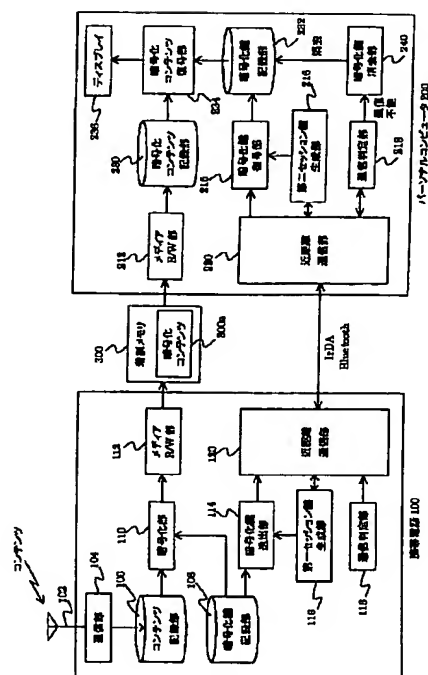
NA41 PA02 PA14

(54) 【発明の名称】 コンテンツ記録システム、コンテンツ転送装置、方法、プログラムおよび該プログラムを記録した記録媒体

(57) 【要約】

【課題】 コンテンツを携帯電話において記録する場合に、携帯電話の外部にコンテンツを適法に移動可能なコンテンツ記録システムを提供する。

【解決手段】 コンテンツ記録部106に記録されたコンテンツは暗号化部110により暗号化され、着脱メモリ300を介して、暗号化コンテンツ記録部230に転送される。通信判定部218が、携帯電話100と近距離通信可能であると判定すれば、暗号化コンテンツ復号化部234が暗号化コンテンツを復号するので、コンテンツを利用できる。一方、第三者が不法コピーする等した場合は、携帯電話100とパーソナルコンピュータ200は遠く離れ、通信判定部218が携帯電話100と近距離通信不能になる。この場合は、暗号化鍵消去部240が暗号化鍵記録部232に記録された暗号化鍵を消去するので、暗号化コンテンツを復号できず、不法コピーを防止できる。



## 【特許請求の範囲】

【請求項1】暗号化鍵を使用して暗号化された暗号化コンテンツを外部に送出する暗号化コンテンツ送出手段を有するコンテンツ記録装置と、  
前記暗号化鍵を記録する暗号化鍵記録手段、  
前記暗号化鍵記録手段に記録された前記暗号化鍵を使用して前記暗号化コンテンツを復号化する暗号化コンテンツ復号手段、  
前記コンテンツ記録装置と通信が可能か否かを判定する通信判定手段、および前記コンテンツ記録装置と通信が不能であれば、前記暗号化鍵を前記暗号化鍵記録手段から消去する暗号化鍵消去手段、  
を有するコンテンツ転送装置と、  
を備えたコンテンツ記録システム。

【請求項2】請求項1に記載のコンテンツ記録システムであって、  
前記コンテンツ記録装置は、  
前記暗号化鍵を暗号化して外部に送出する暗号化鍵送出手段を有し、  
前記コンテンツ転送装置は、  
暗号化された前記暗号化鍵を復号化して前記暗号化鍵記録手段に出力する暗号化鍵復号手段を有する、  
コンテンツ記録システム。

【請求項3】請求項2に記載のコンテンツ記録システムであって、  
前記コンテンツ記録装置は、  
前記暗号化鍵を暗号化するためのセッション鍵を生成する第一セッション鍵生成手段を有し、  
前記コンテンツ転送装置は、  
前記暗号化鍵を復号化するために前記セッション鍵を生成する第二セッション鍵生成手段を有する、  
コンテンツ記録システム。

【請求項4】請求項1に記載のコンテンツ記録システムであって、  
前記暗号化コンテンツ送出手段は記録媒体に前記暗号化コンテンツを送出し、  
前記暗号化コンテンツ復号手段は前記記録媒体から前記暗号化コンテンツを読み出す、  
コンテンツ記録システム。

【請求項5】暗号化鍵を記録する暗号化鍵記録手段と、  
前記暗号化鍵記録手段に記録された前記暗号化鍵を使用して、前記暗号化鍵を使用して暗号化され外部から転送されてきた暗号化コンテンツを復号化する暗号化コンテンツ復号手段と、  
前記暗号化コンテンツの転送元と通信が可能か否かを判定する通信判定手段と、  
前記暗号化コンテンツの転送元と通信が不能であれば、前記暗号化鍵を前記暗号化鍵記録手段から消去する暗号化鍵消去手段と、  
を備えたコンテンツ転送装置。

【請求項6】暗号化鍵を記録する暗号化鍵記録工程と、  
前記暗号化鍵記録工程において記録された前記暗号化鍵を使用して、前記暗号化鍵を使用して暗号化され外部から転送されてきた暗号化コンテンツを復号化する暗号化コンテンツ復号工程と、  
前記暗号化コンテンツの転送元と通信が可能か否かを判定する通信判定工程と、  
前記暗号化コンテンツの転送元と通信が不能であれば、前記暗号化鍵を消去する暗号化鍵消去工程と、  
を備えたコンテンツ転送方法。

【請求項7】暗号化鍵を記録する暗号化鍵記録処理と、  
前記暗号化鍵記録処理において記録された前記暗号化鍵を使用して、前記暗号化鍵を使用して暗号化され外部から転送されてきた暗号化コンテンツを復号化する暗号化コンテンツ復号処理と、  
前記暗号化コンテンツの転送元と通信が可能か否かを判定する通信判定処理と、  
前記暗号化コンテンツの転送元と通信が不能であれば、前記暗号化鍵を消去する暗号化鍵消去処理と、  
をコンピュータに実行させるためのプログラム。

【請求項8】暗号化鍵を記録する暗号化鍵記録処理と、  
前記暗号化鍵記録処理において記録された前記暗号化鍵を使用して、前記暗号化鍵を使用して暗号化され外部から転送されてきた暗号化コンテンツを復号化する暗号化コンテンツ復号処理と、  
前記暗号化コンテンツの転送元と通信が可能か否かを判定する通信判定処理と、  
前記暗号化コンテンツの転送元と通信が不能であれば、前記暗号化鍵を消去する暗号化鍵消去処理と、  
をコンピュータに実行させるためのプログラムを記録したコンピュータによって読み取り可能な記録媒体。

## 【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、コンテンツの適法な移動および利用に関する。

【0002】

【従来の技術】近年、携帯電話を使用し、インターネットや無線回線を介してコンテンツを購入することが行なわれている。ここで、購入したコンテンツは携帯電話に内蔵されている内蔵メモリに記録される。

【0003】また、購入したコンテンツは、着脱式のメモリ（メモリスティック等）には移動させることはできないように設定されている。購入したコンテンツを着脱式のメモリに移動させることができれば、コンテンツを購入していないユーザの所有する携帯電話の内蔵メモリにもコンテンツを移動させることができ、不法コピーを誘発するからである。

【0004】

【発明が解決しようとする課題】しかしながら、携帯電話の内蔵メモリの容量には限界がある。よって、コンテ

ンツを大量に購入した場合、内蔵メモリに記録しきれない場合がある。したがって、既に入力したコンテンツを内蔵メモリから消去して、内蔵メモリの空き容量を確保しなければ、コンテンツを大量に購入することができない場合がある。ここで、既に入力したコンテンツを長く保存したいとユーザが願っても、内蔵メモリの空き容量確保のために、既に入力したコンテンツを廃棄しなければならないといった事態が生じる。既に入力したコンテンツを着脱式のメモリに移動することはできないので、既に入力したコンテンツを保存しておくことはできない。

【0005】そこで、本発明は、購入されたコンテンツを携帯電話等において記録する場合に、携帯電話等の外部に購入されたコンテンツを適法に移動させることができるコンテンツ記録システム等を提供することを課題とする。

【0006】

【課題を解決するための手段】本発明は、コンテンツ記録システムに関する。本発明にかかるコンテンツ記録システムは、コンテンツ記録装置とコンテンツ転送装置とを有する。

【0007】コンテンツ記録装置は、暗号化鍵を使用して暗号化された暗号化コンテンツを外部に送出する暗号化コンテンツ送出手段を有する。

【0008】コンテンツ転送装置は、暗号化鍵記録手段、暗号化コンテンツ復号手段、通信判定手段、暗号化鍵消去手段を有する。

【0009】暗号化鍵記録手段は暗号化鍵を記録する。暗号化コンテンツ復号手段は、暗号化鍵記録手段に記録された暗号化鍵を使用して暗号化コンテンツを復号化する。通信判定手段は、コンテンツ記録装置と通信が可能か否かを判定する。暗号化鍵消去手段は、コンテンツ記録装置と通信が不能であれば、暗号化鍵を暗号化鍵記録手段から消去する。

【0010】上記のように構成された発明によれば、コンテンツ転送装置とコンテンツ記録装置とが通信可能であれば暗号化コンテンツを復号化して利用できる。よって、購入等されたコンテンツをコンテンツ記録装置から外部に移動させて利用できる。

【0011】一方、コンテンツ転送装置とコンテンツ記録装置とが通信不能となればコンテンツ転送装置に記録された暗号化鍵は消去されてしまう。よって、コンテンツ転送装置に記録された暗号化コンテンツを利用できない。したがって、コンテンツ転送装置に転送された暗号化コンテンツが第三者にコピーされても利用できず、不法コピーを防止できる。

【0012】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。

【0013】図1は、本発明の実施形態にかかる携帯電

話100のハードウェアブロック図である。携帯電話100は、CPU2、ディスプレイ5、RAM6、ROM7、VRAM8、アンテナ102、通信部104、メディアR/W部112、近距離通信部120を備える。

【0014】CPU2は、各部を制御する。ディスプレイ5は、VRAM8から表示用のデータを読み出して表示する。RAM(Random Access Memory)6は、読み書き可能なメモリである。ROM(Read Only Memory)7は、読み込みだけが可能なメモリである。VRAM(Video RAM)8は、表示用のデータが書き込まれるメモリである。アンテナ102は、電磁波を送り、または受ける。通信部104は、アンテナ102に結合され通信を行なう。メディアR/W部112は、着脱メモリ300などの記録媒体(メディア)から情報を読み込む(Read)または書き込む(Write)。なお、着脱メモリ300には、スティックメモリなどがある。近距離通信部120は、IrDA、Bluetoothなどにより近距離通信を行なう。近距離通信部120が通信可能な距離は、通信部104が通信可能な距離よりもかなり小さい。

【0015】なお、これらの各部はバスにより連結されている。また、携帯電話100はこの他にも多くの機能を有するが、図1においては図示省略する。

【0016】図2は、本発明の実施形態にかかるパーソナルコンピュータ200のハードウェアブロック図である。パーソナルコンピュータ200は、CPU3、RAM12、ROM13、VRAM14、メディアR/W部212、近距離通信部220、ディスプレイ236を備える。

【0017】CPU3は、各部を制御する。RAM(Random Access Memory)12は、読み書き可能なメモリである。ROM(Read Only Memory)13は、読み込みだけが可能なメモリである。VRAM(Video RAM)14は、表示用のデータが書き込まれるメモリである。メディアR/W部212は、着脱メモリ300などの記録媒体(メディア)から情報を読み込む(Read)または書き込む(Write)。なお、着脱メモリ300には、スティックメモリなどがある。近距離通信部220は、IrDA、Bluetoothなどにより近距離通信を行なう。近距離通信部220が通信可能な距離は、通信部104(図1参照)が通信可能な距離よりもかなり小さい。ディスプレイ236は、VRAM14から表示用のデータを読み出して表示する。

【0018】なお、これらの各部はバスにより連結されている。また、パーソナルコンピュータ200はこの他にも多くの機能を有するが、図2においては図示省略する。

【0019】図3は、本発明の実施形態にかかる携帯電話(コンテンツ記録装置)100およびパーソナルコンピュータ200(コンテンツ転送装置)の構成を示すブロック図である。なお、携帯電話(コンテンツ記録装

置) 100およびパーソナルコンピュータ200(コンテンツ転送装置)がコンテンツ記録システムを構成する。

【0020】携帯電話(コンテンツ記録装置)100は、アンテナ102、通信部104、コンテンツ記録部106、暗号化鍵記録部108、暗号化部(暗号化コンテンツ送出手段)110、メディアR/W部112、暗号化鍵送出手段114、第一セッション鍵生成部116、通信判定部118、近距離通信部120を備える。携帯電話(コンテンツ記録装置)100は、コンテンツを記録する。

【0021】アンテナ102は、図示省略したコンピュータ等からインターネット等のネットワークおよび通信回線等を介してコンテンツを受信する。通信部104は、受信されたコンテンツをコンテンツ記録部106に記録する。すなわち、携帯電話100は、コンテンツをダウンロードする。コンテンツとしては、画像、音声などを記録したファイルが考えられる。ここでは、コンテンツとして画像を記録したファイルを想定する。コンテンツは、携帯電話100の図示省略したディスプレイに表示させることができる。コンテンツ記録部106は、ダウンロードされたコンテンツを記録する。

【0022】コンテンツをダウンロードするという行為は、通常はユーザがコンテンツを購入したということを意味する。このような有償コンテンツは、著作権を販売元が放棄していないことが多い。そこで、第三者がコンテンツをコピーしてしまうと不法コピーとなることが多い。

【0023】暗号化鍵記録部108は、コンテンツを暗号化するための暗号化鍵を記録する。暗号化部110は、コンテンツ記録部106に記録されたコンテンツを、暗号化鍵記録部108に記録された暗号化鍵を使用して暗号化コンテンツを出力する。なお、暗号化の方法としては、例えばDES(Data Encryption Standard)などを使用できる。また、暗号化する方法としてDESを使用することができるという記載は、これ以降は省略する。また、暗号化部110は、後述するようにメディアR/W部112を介して外部(着脱メモリ300)に暗号化コンテンツを送出する。すなわち、暗号化部110は、暗号化コンテンツ送出手段に相当する。メディアR/W部112は、暗号化部110が出力する暗号化コンテンツを、着脱メモリ300に書き込む。着脱メモリ300は、暗号化コンテンツ300aを記録する。

【0024】暗号化鍵送出手段114は、暗号化鍵記録部108から暗号化鍵を読み出し、第一セッション鍵生成部116が生成したセッション鍵により暗号化する。そして近距離通信部120を介してパーソナルコンピュータ200に送信する。第一セッション鍵生成部116は、携帯電話100およびパーソナルコンピュータ200が、近距離通信により認証を行なう際にセッション鍵

を生成して、暗号化鍵送出手段114に出力する。

【0025】通信判定部118は、パーソナルコンピュータ200の通信判定部218(後述)からの通信確認に近距離通信部120を介して応答する。近距離通信部120は、暗号化鍵送出手段114、第一セッション鍵生成部116および通信判定部118と、パーソナルコンピュータ200との間で、IrDA、Bluetoothなどにより近距離通信を行なう。

【0026】パーソナルコンピュータ(コンテンツ転送装置)200は、メディアR/W部212、暗号化鍵復号部215、第二セッション鍵生成部216、通信判定部218、近距離通信部220、暗号化コンテンツ記録部230、暗号化鍵記録部232、暗号化コンテンツ復号部234、ディスプレイ236、暗号化鍵消去部240を備える。パーソナルコンピュータ(コンテンツ転送装置)200は、携帯電話(コンテンツ記録装置)100から暗号化されたコンテンツが転送される。すなわち、携帯電話(コンテンツ記録装置)100は、暗号化コンテンツの転送元である。

【0027】メディアR/W部212については、後述する。

【0028】暗号化鍵復号部215は、近距離通信部220を介して受信した、セッション鍵により暗号化された暗号化鍵を読み込む。そして、第二セッション鍵生成部216が生成したセッション鍵により、暗号化された暗号化鍵を復号化して暗号化鍵記録部232に出力する。第二セッション鍵生成部216は、携帯電話100およびパーソナルコンピュータ200が、近距離通信により認証を行なう際にセッション鍵を生成して、暗号化鍵復号部215に出力する。なお、セッション鍵は、第一セッション鍵生成部116の生成するセッション鍵と共通するものである。

【0029】通信判定部218は、携帯電話100の通信判定部118に対し、所定の信号を接続確認のために近距離通信部220を介して送信する。そして、通信判定部218から所定時間内に応答があるか否かを判定する。ここで、所定時間内に応答がなければ、パーソナルコンピュータ200が携帯電話100と通信不能である旨の信号を暗号化鍵消去部240に送る。近距離通信部220は、暗号化鍵復号部215、第二セッション鍵生成部216および通信判定部218と、携帯電話100との間で、IrDA、Bluetoothなどにより近距離通信を行なう。

【0030】メディアR/W部212は、着脱メモリ300に記録された暗号化コンテンツ300aを読み込み、暗号化コンテンツ記録部230に出力する。暗号化コンテンツ記録部230は、メディアR/W部212が出力した暗号化コンテンツを記録する。暗号化鍵記録部232は、暗号化鍵復号部215が出力する暗号化鍵を記録する。暗号化コンテンツ復号部234は、暗号化鍵

記録部 232 に記録された暗号化鍵を使用して、暗号化コンテンツ記録部 230 に記録された暗号化コンテンツを復号する。ディスプレイ 236 は、暗号化コンテンツ復号部 234 が出力するコンテンツを表示する。暗号化鍵消去部 240 は、通信判定部 218 から、パーソナルコンピュータ 200 が携帯電話 100 と通信不能である旨の信号を受けると、暗号化鍵記録部 232 に記録された暗号化鍵を消去する。

【0031】なお、着脱メモリ 300 のかわりに、有線通信を利用して、携帯電話 100 から暗号化コンテンツをパーソナルコンピュータ 200 へ受け渡すようにしてもよい。また、近距離通信部 120、220 を有線にて連結し通信を行なうようにしてもよい。

【0032】次に、本発明の実施形態の動作を説明する。

【0033】図 4 は、携帯電話（コンテンツ記録装置）100 が、コンテンツをダウンロードしてから着脱メモリ 300 に記録するまでの動作を示すフローチャートである。

【0034】まず、コンテンツをアンテナ 102 が受信し、通信部 104 がコンテンツをコンテンツ記録部 106 に出力する。コンテンツ記録部 106 はコンテンツを記録する。すなわち、携帯電話 100 がコンテンツをダウンロードする（S12）。ダウンロードされたコンテンツは、暗号化鍵記録部 108 に記録された暗号化鍵を使用して、暗号化部 110 により暗号化される（S14）。暗号化部 110 は、暗号化コンテンツをメディア R/W 部 112 を介して着脱メモリ 300 に書き込む（S16）。

【0035】図 5 は、パーソナルコンピュータ 200 が、コンテンツの転送を受ける準備処理からコンテンツの利用までの動作を示すフローチャートである。

【0036】まず、携帯電話 100 とパーソナルコンピュータ 200 とを近づけ、第一セッション鍵生成部 116 と第二セッション鍵生成部 216 とが認証のための通信を行ない、共通のセッション鍵を生成する（S22、S32）。携帯電話 100 においては、暗号化鍵送出部 114 が暗号化鍵をセッション鍵により暗号化する（S24）。そして、セッション鍵により暗号化された暗号化鍵は、近距離通信部 120 を介してパーソナルコンピュータ 200 の近距離通信部 220 に送信される（S26）。

【0037】近距離通信部 220 は、セッション鍵により暗号化された暗号化鍵を受信する。そして、暗号化鍵復号部 215 はセッション鍵により暗号化鍵を復号する（S36）。復号された暗号化鍵は暗号化鍵記録部 232 に記録される。ここで、着脱メモリ 300 に記録された暗号化コンテンツ 300a はメディア R/W 部 212 を介して暗号化コンテンツ記録部 230 に記録される。そこで、暗号化コンテンツ復号部 234 は、暗号化コン

テンツ記録部 230 に記録された暗号化コンテンツを、暗号化鍵記録部 232 に記録された暗号化鍵により復号する（S42）。

【0038】ここで、通信判定部 218 は、携帯電話 100 の通信判定部 118 に対し、所定の信号を接続確認のために近距離通信部 220 を介して送信する。そして、通信判定部 118 から所定時間内に応答があるか否かを判定する。応答があれば、通信可能ということである。応答がなければ、通信不能ということである。すなわち、通信判定部 218 は携帯電話 100 と通信可能か否かを判定する（S44）。通信が可能であれば（S44、Yes）、復号されたコンテンツをディスプレイ 236 に表示する（S46）。そして、通信可能か否かの判定（S44）に戻る。また、通信判定部 218 は携帯電話 100 と通信不能であれば（S44、No）、その旨を示す信号を暗号化鍵消去部 240 に送る。そして、暗号化鍵消去部 240 は、暗号化鍵記録部 232 に記録された暗号化鍵を消去する（S48）。暗号化鍵が消去されれば、暗号化コンテンツの復号ができない。よって、処理は終了する。なお、任意の時点において、パーソナルコンピュータ 200 の電源を断つ（S50）ことによっても処理は終了する。

【0039】本発明の実施形態によれば、パーソナルコンピュータ 200 と携帯電話 100 とが通信可能であれば暗号化コンテンツを復号化してディスプレイ 236 に表示させることにより利用できる。よって、携帯電話 100 のユーザが購入して、携帯電話 100 にダウンロードしたコンテンツを、携帯電話 100 から外部に移動させてパーソナルコンピュータ 200 において利用できる。

【0040】一方、パーソナルコンピュータ 200 と携帯電話 100 とが通信不能となればパーソナルコンピュータ 200 の暗号化鍵記録部 232 に記録された暗号化鍵は消去されてしまう。よって、パーソナルコンピュータ 200 の暗号化コンテンツ記録部 230 に記録された暗号化コンテンツを利用できない。したがって、パーソナルコンピュータ 200 に転送された暗号化コンテンツが第三者にコピーされても利用できず、不法コピーを防止できる。

【0041】通常、携帯電話 100 はユーザが携帯するものであり、第三者は携帯電話 100 を携帯することは一般的には考えられない。そこで、暗号化コンテンツが第三者にコピーされても、コピーされた暗号化コンテンツは、携帯電話 100 から遠く離れていることになる。例えば、インターネットを介して、コピーを不法に伝送する場合は、コピーされたコンテンツは携帯電話 100 から遠く離れていることは明らかである。パーソナルコンピュータ 200 が携帯電話 100 から遠く離れれば、IrDA 等による近距離通信が行なえない。よって、パーソナルコンピュータ 200 に転送された暗号化コンテンツ

が第三者にコピーされても利用できず、不法コピーを防止できる。

【0042】また、携帯電話100からパーソナルコンピュータ200へ暗号化鍵を送信する際に、暗号化鍵がセッション鍵により暗号化する。そこで、暗号化鍵が近距離通信を行なう際に盗まれることを防止できる。

【0043】また、上記の実施形態は、以下のようにして実現できる。CPU、ハードディスク、フラッシュメモリ、メディア（フロッピー（登録商標）ディスク、CD-ROM、メモリスティックなど）読み取り装置を備えたコンピュータのメディア読み取り装置に、上記の各部分を実現するプログラムを記録したメディアを読み取らせて、ハードディスク、フラッシュメモリなどにインストールする。このような方法でも、上記の機能を実現できる。

【0044】

【発明の効果】本発明によれば、コンテンツ転送装置とコンテンツ記録装置とが通信可能であれば暗号化コンテンツを復号化して利用できる。よって、購入等されたコンテンツをコンテンツ記録装置から外部に移動させて利用できる。

【0045】一方、コンテンツ転送装置とコンテンツ記録装置とが通信不能となればコンテンツ転送装置に記録された暗号化鍵は消去されてしまう。よって、コンテンツ転送装置に記録された暗号化コンテンツを利用できない。したがって、コンテンツ転送装置に転送された暗号化コンテンツが第三者にコピーされても利用できず、不法コピーを防止できる。

【図面の簡単な説明】

【図1】本発明の実施形態にかかる携帯電話100のハードウェアブロック図である。

【図2】本発明の実施形態にかかるパーソナルコンピュータ200のハードウェアブロック図である。

【図3】本発明の実施形態にかかる携帯電話（コンテンツ記録装置）100およびパーソナルコンピュータ200

（コンテンツ転送装置）の構成を示すブロック図である。

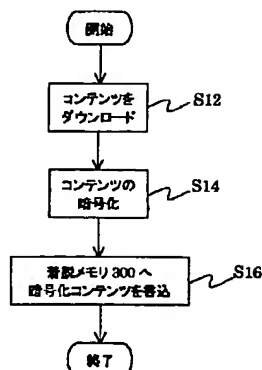
【図4】携帯電話（コンテンツ記録装置）100が、コンテンツをダウンロードしてから着脱メモリ300に記録するまでの動作を示すフローチャートである。

【図5】パーソナルコンピュータ200が、コンテンツの転送を受ける準備処理からコンテンツの利用までの動作を示すフローチャートである。

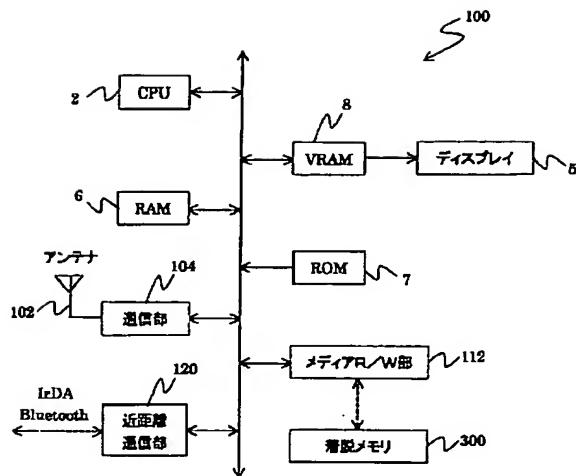
【符号の説明】

- 100 携帯電話（コンテンツ記録装置）
- 102 アンテナ
- 104 通信部
- 106 コンテンツ記録部
- 108 暗号化鍵記録部
- 110 暗号化部
- 112 メディアR/W部
- 114 暗号化鍵送出部
- 116 第一セッション鍵生成部
- 118 通信判定部
- 120 近距離通信部
- 200 パーソナルコンピュータ（コンテンツ転送装置）
- 212 メディアR/W部
- 215 暗号化鍵復号部
- 216 第二セッション鍵生成部
- 218 通信判定部
- 220 近距離通信部
- 230 暗号化コンテンツ記録部
- 232 暗号化鍵記録部
- 234 暗号化コンテンツ復号部
- 236 ディスプレイ
- 240 暗号化鍵消去部
- 300 着脱メモリ
- 300a 暗号化コンテンツ

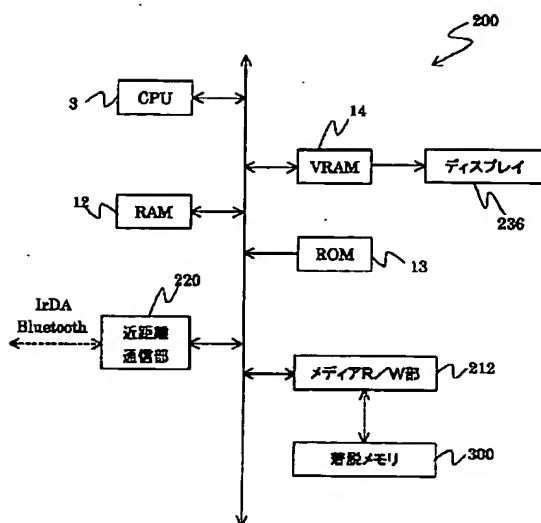
【図4】



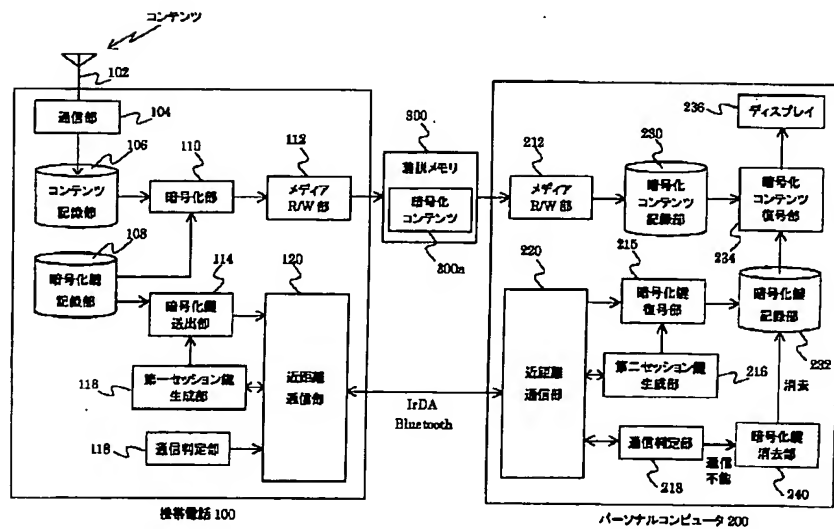
【図1】



【図2】



【図3】



【図5】

